# مروری بر امنیت محیط های رایانش ابری و انواع سیستم های تشخیص نفوذ ابری

---

استاد مربوطه : خانم دکتر لاریجانی
دانشجو: محدثه سادات موسوی

# چکیده:

با فراگیر شدن رایانش ابری و محبوبیت انواع نرم افزار بعنوان سرور و اهمیت آن در انتقال اطلاعات روزانه،امنیت رایانش ابری مهم و مهم تر شده است.افزایش امنیت در هر یک از مدل های رایانش ابری از اهمیت بسزایی برخوردار است.بنابراین تشخیص نفوذ شبکه به عنوان یکی از چالش انگیزترین نیاز های امنیتی شبکه در سال های اخیر درآمده است.سیستم های تشخیص نفوذ با تشخیص و یا پیشگیری از حملات در شبکه های کامپیوتری به افزایش امنیت کمک میکند و نقش موثری در تامین امنیت دارند.

با توجه به افزایش ویروسها و حملات حجم هشدارهای تشخیص نفوذ نیز بسیار بیشتر شده است . از آنجا که محیط های رایانش ابری به دلیل ویژگی توزیع شدگی به راحتی مورد حمله نفوذگر ها قرار میگیرد، استفاده از سیستم های تشخیص نفوذ در ابر یکی از مهمترین راهکارهای امنیتی برای کاهش این تهدیدها میباشد

# مقدمه:

رایانش ابری نوعی سیستم موازی و توزیعی از رایانه های متصل بهم و مجازی است که به صورت پویا و بر اساس توافقات سطح سرویس و به عنوان یک یا چند منبع محاسباتی مجتمع ارائه می.شود رایانش ابری به معنای انتقال پویای منابع و قابلیتهای فناوری اطلاعات به عنوان سرویس روی اینترنت است. صنعت رایانش ابری اکوسیستم بزرگی از مدل ها فروشندگان و بازارهای مختلف است . خدمات رایانشی پنج ویژگی کلیدی و چهار مدل استقرار و سه مدل خدمات دارد

پنج مشخصه اصلی شامل: تجمیع منابع ،دسترسی وسیع از طریق شبکه ،انعطاف پذیری سریع، سرویس خودکار مبتنی بر تقاضا و سرویس اندازه گیری شده باشند. سه مدل خدمات عبارتند از : زیرساخت به عنوان سرویس، پلتفرم به عنوان سرویس و نرم افزار به عنوان سرویس

انواع مدل عرضه شامل ابر خصوصی ابر انجمنی ابر عمومی و ابر هیبرید است. در نمایش دیاگرام شبکه های کامپیوتری بطور معمول از شکل یک ابر به عنوان روشی تلخیصی برای پنهان کردن زیر ساخت های پیچیده ای که درون شبکه وجود دارد استفاده میگردد در رایانش ابری نیز کلمه "ابر" از همین استعاره گرفته شده است و برای پنهان کردن اینترنت و زیرساختها در رایانش ابری نیز بکار میرود

# آشنایی با مفهوم رایانش ابری:

رایانش ابری مدل محاسباتی بر پایه شبکه های بزرگ کامپیوتری مانند اینترنت است که الگویی تازه برای عرضه، مصرف و تحویل سرویس فناوری اطلاعات شامل سخت افزار، نرم افزار ،اطلاعات و سایر منابع اشتراکی محاسباتی با بکارگیری اینترنت ارایه میکند.رایانش ابری راهکارهایی برای ارایه خدمات فناوری اطلاعات به شیوه های مشابه با صنایع همگانی آب، برق . تلفن و ... پیشنهاد می.کند. این بدین معنی است که دسترسی به منابع فناوری اطلاعات در زمان تقاضا و بر اساس میزان تقاضای کاربر به گونه ای انعطاف پذیر و مقیاس پذیر است که از راه اینترنت به کاربر تحویل داده می شود

دلیل تشبیه اینترنت به ابر در این است که اینترنت همچون ابری جزییات فنی اش را از دید کاربران پنهان می سازد و لایه ای از انتزاع را بین این جزییات فنی و کاربران به وجود میاورد به عنوان مثال آنچه یک ارایه دهنده سرویس نرم افزاری رایانش ابری ارایه میکند برنامه های کاربردی تجاری برخط است که از طریق مرورگر وب یا نرم افزارهای دیگر به کاربران ارایه می شود. نرم افزارهای کاربردی و اطلاعات روی سرورها ذخیره می گردند و بر اساس تقاضا در اختیار کاربران قرار می گیرند. جزییات از دید کاربر مخفی میماند و کاربران نیازی به تخصص یا کنترل در مورد فناوری زیر ساخت ابری که از آن استفاده میکنند ندارد

# آشنایی با مفهوم رایانش ابری:

رایانش ابری تکنولوژی است که از سوی شرکتهای مختلفی که مهمترین آنها مایکروسافت گوگل و آمازون می باشند به جهان عرضه شده است. به بیان دیگر این تکنولوژی همان بکارگیری منابع نرم افزاری و سخت افزاری موجود بر روی سرور توسط کاربر میباشد که کاربر را از به روز رسانی مداوم سخت افزار و نرم افزار سیستم خود بی نیاز می سازد. با استفاده از این فناوری تنها نیاز دارید از یک بستر با سرعت مناسب و امنیت بالا جهت دسترسی به سرور استفاده نمایید. در حال حاضر دنیای فناوری اطلاعات قسمت اعظمی از زندگی بشر را در بر میگیرد که در کنار آن این فناوری نیازهایی مانند امنیت اطلاعات دسترسی سریع و آسان در هر لحظه پردازش با قدرت بالا و مهمتر از آن استفاده از سرویس های با هزینه پایین می باشد

پیدایش محیط رایانش ابری ویژگیها و مزایای زیادی در اختیار کاربران قرار داده است.

# ساختار رایانش ابری:

وقتی از پردازش به صورت یک ابر سخن میگوییم بهتر است که ابررایانه ای را متشکل از دو قسمت ابتدایی و انتهایی فرض کنیم که توسط یک شبکه به یکدیگر متصل میگردند و بطور معمول این شبکه همان اینترنت می باشد. بخش ابتدایی قسمتی است که قابل مشاهده کاربران بوده و در برگیرنده اطلاعات و شکل ظاهری نرم افزارها میباشد بخش انتهایی نیز همان .ابر رایانه ای .است که عملیات پردازش را در بر می گیرد نرم افزار مرتبط کننده دو بخش نیز جزئی از بخش ابتدایی میباشد بخش انتهایی یا ابر، از چندین رایانه مرورگر و واحدهای ذخیره کننده اطلاعات تشکیل شده است و از نظر نرم افزاری دارای هرگونه نرم افزاری می‌تواند باشد.

# انواع رایانش ابری:

۱-نرم افزار بعنوان سرویس
۲-پلتفرم بعنوان سرویس
۳-زیر ساخت بعنوان سرویس

# مزایا رایانش ابری:

مزایای اصلی رایانش ابری عبارتند از :

۱-هزینه

۲-مقیاس پذیری

۳-امنیت

۴-نگهداری

۵-عدم وابستگی به تجهیزات خاص و مکان خاص

۶-چند مستاجری

۷-سنجش پذیری و صرفه جویی در مصرف منابع و هزینه ها

# امنیت رایانش ابری:

محیط ابر مهمترین مثال از رایانش توزیع شده است که همه انواع خدمات برای کاربر فراهم شده ارائه دهندگان خدمات زیر ساخت ابر اقدامات امنیتی اولیه در سطح زیرساخت مانند فایروالها حفاظت از انواع مختلف ویروسها را با توسعه و بروزرسانی نرم افزار آنتی ویروس بصورت منظم انجام میدهند ماشینهای مجازی نصب شده روی سیستم عامل امنیت را به روشهای مختلف فراهم میکند با این حال حملات شبکه در مواجه شدن با ماشینهای مجازی شبکه نمی توانند با فایروالها با انتی ویروسها رفع شوند بنابراین یک بررسی در سیستم امنیتی شبکه جهانی در سطح مرکز داده لازم است. بسیاری چارچوب های زیر ساخت ابر وجود دارد که خدمات رایانش ابری و خدمات مجازی سازی را برای کاربر فراهم می کند مانند Cloud Sigma،Cloud Stack ، OpenNode اکالیپتوس، EMOTIV،( مدیریت انعطاف پذیر وظایف در محیط های مجازی شده ) همانطور که منافع و مزایای قابل توجه و غیر قابل انکاری در رایانش ابری وجود دارد. این فناوری شامل ریسکها و مخاطرات مربوط به خود هم میباشد محرمانگی قابلیت اعتماد جامعیت قابلیت دسترسی، قابلیت اعتبار تشخیص هویت و حریم خصوصی اصلی ترین نگرانی ها برای ارائه دهندگان و مصرف کنندگان ابر هستند .ولی بزرگترین نگرانی در بکارگیری رایانش ابری به امنیت مربوط است و پیوسته از مهمترین چالش های این فناوری بوده. بنابراین امنیت بیش از مزایای آن ذینفعان را دچار تردید می کند. امنیت یک چالش برجسته میان سایر چالشها است. طبق تحقیقهای انجام گرفته روی معماریهای امنیتی رایانش ابری کاربران احساس امنیت و اطمینان دارند زمانیکه واقعا بدانند که عملیات چطور در حال انجام و اجرا شدن باشد.

# تهدیدها و حملات ابر:

۱-حمله DoS:
یا از کار اندازی سرویس، نوعی حمله است که هدف آن از کاراندازی سیستم با استفاده از هدر دادن منابع آن است.
بطوریکه سرویس دهنده توانایی سرویس دهی عادی به کاربران مجاز را از دست بدهد.هدف از حملات رد سرویس، غیر قابل دسترس کردن منابع کامپیوتر از کاربرانی که قصد دستیابی به آن را دارند میباشد
۲-حملات DDoS
حملات DDoS نیز مشابه DoSهستند با این تفاوت که حمله از طریق چندین سیستم و بصورت توزیع شده است.
DoSتوزیع شده حمله ای است که اغلب هزاران یا حتی میلیونها کامپیوتر به یک هدف حمله میکنند معمولا مهاجم از تعدادی کامپیوتر بدون اجازه مالکشان که botnetنامیده میشود استفاده میکند
۳-حمله سیل آسا Flooding Attack
۴- XSS:روش نفوذ و گرفتن دسترسی غیر مجاز از یک وب گاه توسط هکرها می باشد.
۵- حملات ماسک: در این حملات تهدیدها نقش کاربران مجاز را بازی می کنند.
۶- حملات مبتنی بر میزبان این حملات نتیجه حملات ماسک و عموما در ناهنجاری رفتاری کاربران قابل مشاهده است

## راهکار های امنیت ابر:

۱-ایجاد زیرساخت کلید عمومی(PKI)روی هر لایه.
۲-استفاده از سیستم تشخیص نفوذ شبکه در ابر
۳-مجازی سازی
۴-راه حل حملات سیل اسا

# مفهوم سیستم تشخیص نفوذ:

سیستم تشخیص نفوذ ،ابزار امنیتی است که هدف آن تقویت امنیت اطلاعات و سیستمهای ارتباطیاز طریق نظارت شبکه یا فعالیتهای سیستم، شناسایی نفوذها و تهیه گزارش می باشد . سیستم های تشخیص نفوذ با مطالعه رفتار
کاربران و اطلاعات موجود در حملات،رفتارهای غیر نرمال را تشخیص می دهند.این سیستم ها معایب و مزایای خاص خود رادارند که با تشخیص و یا پیشگیری از حملات نقش مؤثری در تامین امنیت دارند
IDS های فعال سیستم های جلوگیری از نفوذ IPS هستند که علاوه بر نظارت ترافیک شبکه می توانند از ورود ترافیک ناهنجار به شبکه جلوگیری وتهدیدها رامسدود یا متوقف سازند.

# روش های تشخیص در IDS:

روش تشخیص در سیستم های تشخیص نفوذ برحسب تکنولوژیهای تحلیلی،به دو روش مختلف است:
-تشخیص ناهنجاری
-روش مبتنی بر امضا

# مقایسه IDS ها :

جدول۲- مقایسه سیستم های تشخیص نفوذ مبتنی بر ابر

| Ref. | IDS Name | IDS Type | IPS | Cloud | Snort | Scalable | Real Time | Log file Check | Behavior-based | Knowledge-based | Techniques | | | | | Attack Detection | | | | | | Detection Type | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Data mining | Neural Network | Machine learning | Profiling | Clustering | DoS / DDoS | XSS | TCP SYN Flooding | Packet Flooding | Masquerade | Host-based | Signature | Anomaly |
| (Holtz et al, ۲۰۱۱) | | HIDS NIDS | | ✓ | | ✓ | ✓ | ✓ | | | | | | | | | | | | | | ✓ | |
| (Taghavi Zargar et al, ۲۰۱۱) | DCDIDP | HIDS NIDS | ✓ | ✓ | | | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | | ✓ | | | | | | ✓ | ✓ |
| ( Manavi et al, ۲۰۱۲) | SVL-IDS | HIDS | ✓ | ✓ | | | | | | | | | | | | ✓ | | | | | | | ✓ |
| ( Sathya and Vasanthraj, ۲۰۱۳) | MultiLevel-IDS | NIDS | | ✓ | | | | ✓ | | | ✓ | | | | | | | | | | | | ✓ |
| ( Kholidy and Baiardi, ۲۰۱۲) | CIDS | HIDS NIDS | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | | | | | | | | ✓ | | ✓ | ✓ |
| (He et al, ۲۰۱۲) | | HIDS NIDS | | ✓ | | | ✓ | ✓ | ✓ | | | | ✓ | | ✓ | | | | | | | ✓ | ✓ |
| ( Gupta and Kaliyar, ۲۰۱۳) | BIDS | HIDS NIDS | | ✓ | | | | ✓ | ✓ | | | | | | | ✓ | ✓ | | | ✓ | ✓ | | ✓ |
| ( Gupta et al, ۲۰۱۳) | PIDS | NIDS | ✓ | ✓ | | | | | ✓ | | | | | ✓ | | ✓ | | ✓ | ✓ | | | ✓ | ✓ |

## نتیجه گیری:

مهمترین چالش رایانش ابری تضمین امنیت داده های موجود می باشد.
درحال حاضر حفاظت ازکارکرد ابر در اینترنت یک چالش بزرگ محسوب میشود و راه حل های بسیاری برای امنیت داده ها در رایانش ابری به کار گرفته میشود.همانطور که گفته شد روش های گوناگونی جهت مقابله با حمله های احتمالی ابداع شده اند. به نحوی که ارائه دهندگان ابر از بابت حفاظت داده های شخصی و سازمانی کاربران آسوده باشند